moz://a

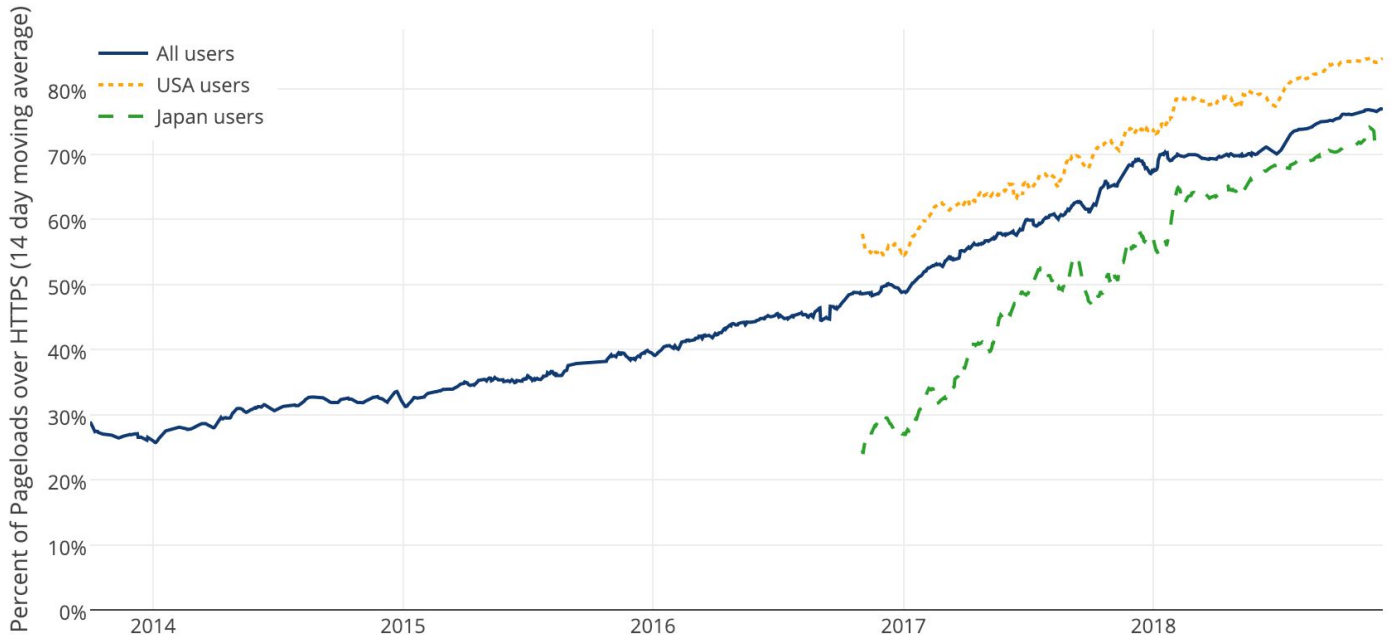
Making HTTPS Revocations Work - CRLite

Crypto Engineering
MGoodwin, JCJ, DPatel

HTTPS Everywhere

Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)



A **certificate** testifies the **server** is valid for **website**

Certificates are supposed to be **revocable**

Standard revocation forms:

OCSP **CRLs**

CRLs

Large. Irrelevant Info.

Firefox uses **OCSP** today

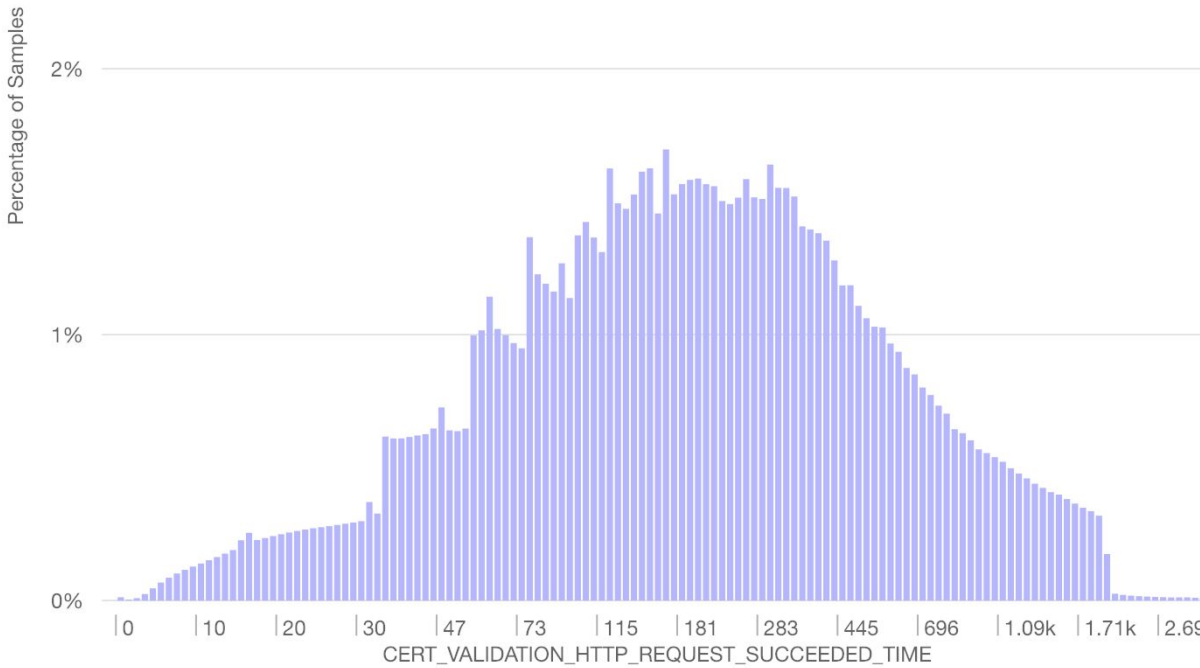
OCSP downsides:

Privacy. Latency.

200 ms to first connection!

Histogram Type	exponential
Ping Count	299.02M
Sample Count	9.97B
Sample Sum	3.54T
Number of dates	159
Selected Dates	2018/06/26 to 2018/12/02

5th Percentile	29.08
25th Percentile	90.72
Median	195.23
75th Percentile	409.76
95th Percentile	1.18k



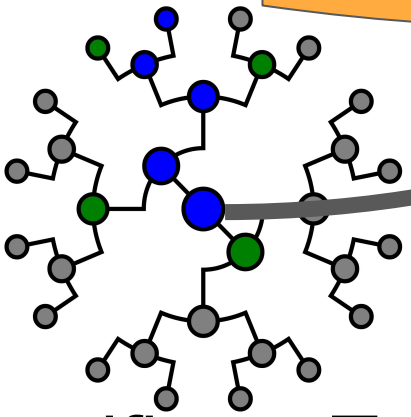
CERT_VALIDATION_HTTP_REQUEST_SUCCEEDED_TIME

CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers

James Larisch* David Choffnes* Dave Levin†
Bruce M. Maggs‡ Alan Mislove* Christo Wilson*
* Northeastern University † University of Maryland ‡ Duke University and Akamai Technologies

...compress and ship all **CRLs**.

Cascading bloom filters



Certificate Transparency

CRLs


Cascading
bloom filters
CT
CRLs

Updates: 100s kB per day

Replace OCSP for the common case

Better privacy

Better latency

Doing it the Mozilla way

CRLite

Experiments in Nightly

Beginning Q1

moz://a Crypto Engineering

:MGoodwin, :JCJ, :DPatel